Quantum Key Distribution

R.J. Hughes, J.E. Nordholt, C.G. Peterson, W.R. Scarlett, J. Anaya, D. Derkacs, J. Franken, P. Hiskett, W.J. Marshall, R. Sedillo, C. Wipf (P-21), K.P. McCabe, I. Bernstein, N. Dallman, I. Medina, P. Montano, N. Olivas, S. Storms, J. Thrasher, K. Tyagi, R.M. Whitaker (ISR-4), J. Wren (ISR-2), P. Milonni (T-DO), J.M. Ettinger, M. Neergaard (N-3), D. Ranken, R. Gurule (CCN-12)

On April 27, 1986, a satellite television broadcast to the east coast of the U.S. was briefly taken over by a hacker calling himself "Captain Midnight." With the growing reliance on satellites for communications, this notorious incident highlights the importance of assured command and control of orbital assets, as well as protection of downlinked data. In 1994, two LANL researchers, Richard Hughes and Jane Nordholt, set out a methodology whereby QKD using single-photon transmissions could be used to provide greater long-term security, based on fundamental principles of quantum physics, for secure satellite communications. Since then, our QKD team has been conducting research toward that goal, and we have developed another secure communications concept that would become possible with a satellite QKD capability—secure data dissemination between dynamically reconfigurable networks of users.[1] This research is leading to QKD becoming a higher-security alternative to present-day public-key-cryptography-based methods of establishing secure communication—today's public-key broadcasts, which we must assume are being recorded by adversaries, will become retroactively vulnerable if a large-scale quantum computer becomes feasible in the future, potentially allowing an adversary access to still-valuable information.

The Basics of Cryptography

The science of cryptography provides two parties ("Alice" and "Bob") with the ability to communicate with long-term *confidentiality*—they have the assurance that any third party (an eavesdropper, "Eve") will not be able to read their messages. Alice can encrypt a message ("plaintext"), P, before transmitting it to Bob, using a cryptographic algorithm, E, to produce a "ciphertext," C, which depends on K, a secret parameter known as a cryptographic key. [K is a random binary number sequence, typically a few hundred bits in length. For example, in the Advanced Encryption Standard the keys are up to 256 bits in length.] Bob is able to invert the encryption process to recover the original message, P, provided he too knows the secret key, K. Although the encryption algorithm E may be publicly known, Eve passively monitoring transmission C would be unable to discern the underlying message, P, because of the randomization introduced by the encryption process—provided the cryptographic key, K, remains secret. (The algorithm E is designed so that without knowledge of K, Eve's best strategy is no better than an exhaustive search over all possible keys—a computationally infeasible task.) In this so-called *symmetric key* cryptography, *secret* key material is therefore a very valuable resource, but there is an underlying problem; before Alice and Bob can communicate securely it is of paramount importance that they have a method of securely distributing their keys. It is this problem of key distribution that QKD solves, providing the ultimate security assurance of the laws of physics (Figure 1).

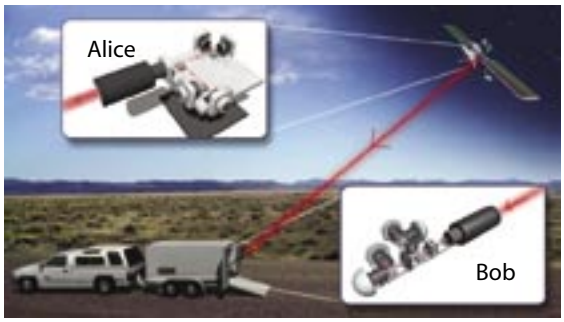


Figure 1. In our conceptual satellite QKD system, the transmitter of the quantum key material (Alice) is on the orbiting satellite and the receiver (Bob) is on the ground. Alice's four attenuated lasers (top left) will transmit polarized photons to Bob's receiving telescope (lower right), which collects them and directs them to one of four detectors. The registered signal from these detectors forms the raw key material for a cryptographic system whose secrecy is guaranteed by the laws of quantum physics.

The QKD Concept

QKD was first proposed in 1984 by Charles Bennett (IBM) and Gilles Brassard (University of Montreal). Alice and Bob, equipped with the ability to perform conventional, nonsecret ("public") but authenticated communications with each other, could produce copious quantities of shared, secret random key bits, for use as cryptographic keys, by using quantum communications. In their "BB84" QKD protocol, Alice (the transmitter) sends a sequence of random bits over a "quantum channel" to Bob (the receiver) that are randomly encoded as linearly polarized single photons in either of two conjugate polarization bases with (0, 1) = (H, V), where "H" ("V") denotes horizontal (vertical) polarization (respectively), in the "rectilinear" basis, or (0, 1) = (+45°, -45°), where "+45°" and "-45°" denote the polarization directions in the "diagonal" basis. Bob randomly analyzes the polarization of arriving photons in either the rectilinear or diagonal basis, assigning the corresponding bit value to detected photons. Then using the public channel, which is assumed to be susceptible to passive monitoring by Eve, he informs Alice in which time slots he detected photons but without revealing the bit value he assigned to each one.

Next, Alice reveals her basis choice for each bit but not the bit value. Bob communicates back the time slots of his detected bits for which he used the same basis as Alice. In an ideal system, Alice's transmitted bits and the results of Bob's measurements on this random, matching-basis portion, known as the "sifted" key, are perfectly correlated; they discard the bits for which Bob used the wrong basis (e.g., his receiver "looked" in the diagonal basis when she transmitted the bits in the rectilinear basis and *vice versa*) (Figure 2).

In practice, Bob's sifted key contains errors. Fundamental quantum principles ensure that Eve is both limited in how much information she may obtain by eavesdropping on the quantum communications and that she cannot do so without introducing errors in Bob's sifted key from which Alice and Bob can deduce a rigorous upper bound on leaked information. Alice and Bob determine this bound after reconciling their sifted keys using *post facto* error correction over their public channel. From their partially secret reconciled keys, Alice and Bob extract the shorter, final *secret* key after a final stage known as "privacy amplification." For example, if Alice and Bob form the parities of suitable random subsets of their reconciled bits, they can be sure that Eve will be ignorant of at least one of the bits in each subset and hence ignorant of the final secret bits.

Free-Space QKD

A satellite-to-ground free-space QKD capability has particularly appealing security features. Typically, satellites are launched with all the keys they will ever have but they may exceed their design lifetime or they may need to encrypt more data than expected. Then one must face the challenge of providing new keys to a possibly very high-value satellite asset on-orbit. Clearly it is infeasible to use a human courier for this task, and although public-key cryptography allows keys to be transferred conveniently, its use already presents a latent vulnerability to unanticipated computation advances, including quantum computers. In contrast, QKD provides much greater long-term security guarantees—it can only be attacked by technology in existence at the time of transmission and cannot be attacked by a quantum computer. A second advantage of QKD is in the context of *key generation*; it allows a fresh key to be produced at transmission time using the intrinsic randomness of quantum mechanics. This could be very useful to support the demands for large amounts of key material within a transformational communications scenario, as well as reducing the risks associated with conventional keys—that they might be (accidentally or maliciously) compromised by insiders. Finally, QKD narrows an adversary's window of opportunity; Eve's best strategy is to attempt a "man-in-the-middle" attack, but to do so she would have to break the initial authentication

in time to insert herself into the channel between Alice and Bob. Breaking the authentication *after* the quantum communications have taken place is of no use to Eve.

For satellite-to-ground (or any other line-of-sight application) QKD, one must reliably transmit and detect single photons through the atmosphere in the presence of background radiance, which is a strong error source even at night. We effectively deal with this challenging problem using a combination of spectral, spatial, and temporal filtering. The synchronization requirements are especially important; we must only accept photons that reach the receiver within specific 1-ns time windows. Our solution to this difficult problem makes QKD possible even in full daylight, which is one of the unique features of our research that sets us apart from our competitors.

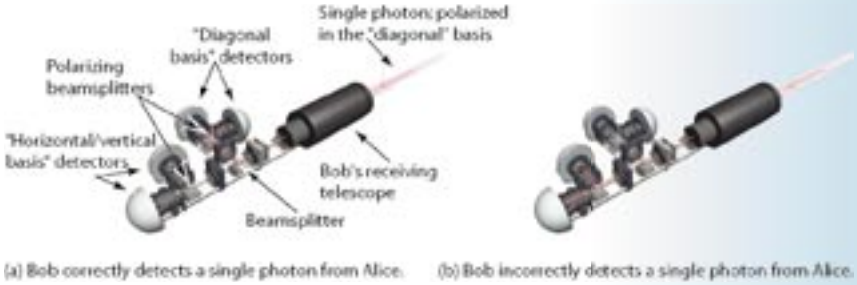
In 2001, using a readily transportable system, we carried out a QKD experiment over a 10-km line-of-sight range between Pajarito Mountain and TA-53, LANL, which had optics (extinction of one air mass, background, and turbulence) representative of a satellite-to-ground path.[2] We were able to reliably produce shared, secret keys at rates of several hundred bits per second throughout the day and night (i.e., 1–2 keys per second). On each clock cycle (1 MHz at the time), the transmitter (Alice) generates two secret random bits, which determine which one of four attenuated "data" diode lasers emits about a 1-ns optical pulse with one of the BB84 polarizations (see the Alice inset in Figure 1) and an average photon number less than one (with Poissonian photon-number statistics) that is launched towards the receiver (Bob). At Bob, a telescope collects the data pulse and directs it into an optical system where its polarization is randomly analyzed in one of the BB84 bases. Single-photon detectors, one for each of the four BB84 polarizations, register the result (see the Bob inset in Figure 1). This process is repeated for one second, following which the session is completed with the various public-channel processes (sifting, reconciliation, and privacy amplification) using a wireless Ethernet connection before starting up the next 1-s session. (In subsequent work using the data from this experiment, we implemented for the first time in QKD research the all-important authentication aspect and demonstrated that self-sustaining, authenticated, secret-key production is possible with minimal overhead in secret bits.) The background rejection in our system was sufficiently high that we were even able to transfer secret key bits under worst-case conditions with the sun directly illuminating the receiver.

Implications and Developments for Satellite QKD

With input from the results of this experiment, we have developed a model that allows free-space QKD performance to be predicted in other regimes. In particular, we have modeled a QKD link between a satellite and a ground location.[3] We have determined that it is optimal to locate the transmitter (Alice) on the satellite and the receiver (Bob) on the ground so that the optical effects of atmospheric turbulence are in the transmitter's far-field zone. For low-earth-orbit (LEO) satellites, we find that useful QKD contacts can be established over wide areas of the earth's surface, day or night, using only modest-scale (~ 50-cm in diameter) optical ground facilities, whereas with larger aperture (> 1-m in diameter) optical ground facilities, QKD from higher altitude orbits (such as geosynchronous ones) would be feasible at night.

We have also developed a preflight QKD transmitter (a so-called "brassboard"). This device is sufficiently small and lightweight that it could be accommodated on a satellite, yet sufficiently rugged that it could survive the rigors of launch. So far, we have tested this in a laboratory environment and produced large quantities of high-quality, secret key

Figure 2. The raw QKD key material must be "sifted" to produce useful, matching bit strings. In this example, Bob is receiving a single photon that Alice transmitted in the "diagonal" basis (see text for details). The first beamsplitter randomly directs the photon either to the right (a) or straight ahead (b). If the photon goes to the right, a second polarizing beamsplitter will direct it to the correct "diagonal basis" detector, and it becomes a useful bit of key material (a "1" or a "0"). If the photon goes straight ahead, another polarizing beamsplitter will randomly send it to a "horizontal/vertical basis" detector—this randomness eliminates its usefulness as key material. Bob communicates with Alice over a public channel how he detected each photon—but not the result. Alice tells Bob which photons were tested correctly, and those bits form the "sifted" cryptographic key.



bits. The performance of this device, together with our modeling results give us great confidence that satellite-to-ground QKD would be possible at useful rates with existing technology.

It is likely that on-orbit re-keying would be performed with a QKD ground unit located at a satellite's operations center or mission-control center, but the modest parameters required of a ground-receive unit (for LEO satellites) suggests another use—the transfer of keys between ground users via a QKD-capable satellite. For example, a QKD capable satellite could generate keys with each of two QKD ground units in different parts of the world (which could be transportable systems). The satellite could then communicate to the second user which bits to flip so that his key matches the first user's; this information could be sent in the clear without compromising security. These ground users could now establish secure communications over any convenient channel using this shared key. Several cross-linked QKD-capable satellites could support worldwide on-demand secure communications to the coalitions of land-, sea-, air-, and space-based users envisioned in emerging "transformational-communications" concepts. This concept can be further extended with optical-fiber QKD links to the satellite QKD ground units. Building on previous work in which we have demonstrated QKD over a 48-km optical-fiber path in LANL's network,[4] we have recently shown the feasibility of the much harder problem of performing QKD over a fiber that is also carrying network traffic.[5] Optical-fiber QKD would therefore not require a dedicated fiber connection.

Conclusion

While considerable basic and applied research remains to be done, QKD is the first aspect of quantum information science to enter the technology-development era; it is possible with existing technology and is capable of providing solutions to the pressing secure-communications requirements of the next decade. The LANL QKD team is in the forefront of this "first wave" of QKD research and development, but we are also engaged in the basic research of the "second wave" of QKD that will be based on the uniquely quantum-mechanical properties of "entangled" two-photon states.

References

1. R.J. Hughes and J.E. Nordholt, "A new face for cryptography," *Los Alamos Science* **27**, 68–85 (2002).
2. R.J. Hughes, J.E. Nordholt, D. Derkacs *et al.*, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics* **4**, 43.1–43.14 (2002).
3. J.E. Nordholt, R.J. Hughes, G.L. Morgan *et al.*, "Present and future free-space quantum key distribution," in *Free-Space Laser Communication Technologies XIV*, G.S. Mecherle, Ed. (SPIE, Bellingham, Washington, 2002), Proceedings of SPIE Vol. 4635, pp. 116–126.
4. R.J. Hughes, G.L. Morgan, and C.G. Peterson, "Quantum key distribution over a 48-km optical fiber network," *Journal of Modern Optics* **47**, 533–547 (2000).
5. P. Tolliver, R.J. Runser, T.E. Chapuran *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photonics Technology Letters* **15**(11), 1669–1671 (2003).

Acknowledgment

It is a pleasure to acknowledge collaborations with P. Kwiat of the University of Illinois; S. Nam, A. Miller, and D. Rosenberg of the NIST; A. Ellsasser, M. Dulski, R. Baker, and R. Trevino of the DoD; R. Blake, S. McNown, P. Hendrickson, R. Shea, and T. Persons of the U.S. government; M. Goodman, R. Runser, T. Chapuran, P. Tolliver, and J. Jackel of Telcordia; and N.C. Donnangelo of The MITRE Corporation. This research was funded by the Advanced Research and Development Activity and the Secretary of the Air Force.

For further information, contact Richard Hughes at 505-667-3876, hughes@lanl.gov, or Jane Nordholt at 505-667-3897, jnordholt@lanl.gov.